ISSN:0975-9646

Counter Measures against Malicious Program in Universal Serial Bus

Selvi Grija[*1], Kovartthan[*2], Selva Kumar[*3], Thamilzselvan[*4]

[*]*Computer Science Department,*
Christ college of engineering and technology,
Pondicherry, India

***Abstract*— USB that are used to transfer the data through computers .It will available in a smaller size to do certain amount of data files. The USB are used as in many format like mass storage devices, etc. where the information security in the universal serial bus due to insecure design the USB can easily attack .The malicious code can exploit the USB drivers and autoplay features to launch various software attacks on host and USB devices .The worms or virus are malware that are replicating through the USB devices and they are attacking the normal function of the operating systems .The purpose is to provide the prevention of replication of the virus to the operating systems and to support the operating system from the attacks of vulnerabilities.**

***Keywords*— Autoplay, Mass storage, Malicious code, USB, Virus, Vulnerability, Worms.**

I. INTRODUCTION

USB is a standard that is used for the communication of the devices with computer largely. It is not used to transfer the files between the users. It is used to connect the devices like printer, dongle etc. to the computers. It has replaced largely the ports that are used to connect the devices like parallel and serial ports. USB used for transferring the data at the rate of high speed to the computers. The USB has the feature of plug and play, it means we can watch or hear the audio to the electronic devices. Virus is a program to create for the destruction purpose of the normal operation of the computer system. Nowadays the virus is attacked through majorly USB pen drives. For example, if a user has virus in his personal computer then he wants to transfer the files to his friend pen drive when he inserts the pen drive the virus was easily replicated to pen drive. Hence the virus moves to other computer very easily without user's knowledge. Antivirus is a tool to remove the virus very easily but still replicated virus can't be stopped. The viruses are replicated when we insert the pen drive to the computer. There are many tools to remove the virus from the operating system or the USB devices from the viruses, but they aren't removed completely The virus are removed by the antivirus they are sent to the quarantine, means the infected files are moved safely, sometimes there is a virus which can't be deleted Even though the device was once attacked there is a probability of damaging or non-working the devices**.** Nowadays the antivirus software didn't allow changing the default system value in registry. There is much software to kill the malware in the universal serial bus devices. In the internet there is a many software to remove the virus in the USB drives .Although the virus was removed it affects the system for at least one time .The famous antivirus software are McaFee, avast ,avg antivirus and Kaspersky are the virus remover that are provided .With these software ,the windows operating system was in built with the windows defender and Microsoft security essentials .Windows Defender is now currently running with the operating system windows 8 .Microsoft essential was stop the service with the windows 7.There is insecure design in USB driver that was provided by the Windows Corporation .

1.1 Universal Serial Bus Attack Based On Software Attacks And Protection

They told about the attacks that are performed in the USB. The viruses like Trojans, worms etc. are exploit the autoplay feature which is provided by the windows operating systems. The autoplay feature will support currently used operating systems. They are used to show the more options of the USB performed in the computers.

1.2 A Survey About the Antivirus technology

Nowadays the scanners are the technology which is used to scan the virus using software provide by top companies. Even they provide a top technology in scanning and deleting the virus when the USB inserted the virus was easily attack by passing the wall provided by them. The virus are developed very strongly even the software are updated regularly.

1.3 Problem faced in inserting the USB

When a user insert his own data it is can't be said it is secure or not .The user uses the USB devices at various systems .We can't say that all systems are secured or disinfected system. Today virus are spreading through the internet and infected system .The infected system consists of any kind of virus .When we insert the USB devices the virus can spread into the USB drive .It can't happen only an individual system it can also happen in host computers. virus are programmed self-replicated when an USB inserted it spread into them, and it can't be deleted .The virus can be removed by an antivirus program that are installed in the computers Here the virus are quarantine that means a antivirus program stop the process that was open by an individual antivirus program .The individual virus can place its executable files in the local disk drive that is hard disk it is main reason for replication of virus program when we inserting the USB drives. So USB said as insecure design to transfer the data. However the software may protect the USB.

II. METHODOLOGY

2.1 Disabling Autoplay Feature

Here first we are disabling the feature in windows called autoplay feature. The autoplay feature will allow you to access the content of USB pen drive by using a wizard. When a infected pen drive is inserted to the computer, the virus called replicating virus. Without opening the pen drive the virus is easily copied to the system. For this autoplay feature is cause to copy the virus to the computer. So we can disable it by changing the value of autoplay feature in the windows . After that we are performing a virus scan in the computer. To check whether there is a virus in the system.

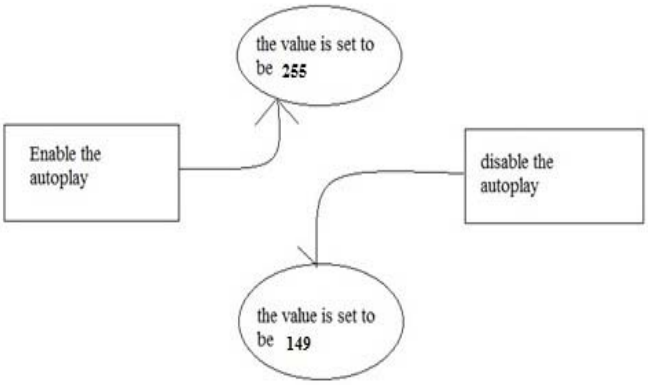

Fig 1 Disable and enable the autoplay

2.2 Enabling USB Read Only Mode

This module enables the system to read the content in the USB. Because the virus are replicated to system when it is connected although we are disabling the autoplay feature. But the pen drive still consists of virus, so we are making the USB pen drive into read only. Hence now it is write protected, the virus can't be copied to the system. USB read only can be enabled in the system by changing the value in the registry editor. The read option can be enabled by changing its value into 0 into 1.The 1 value indicates that the USB can be read only. The value 0 indicates that the USB devices are write only. This feature is used to protect the virus from the infected devices that shouldn't be copied to the system. The virus can be easily copied to the system when it is connected. It can be prevented before it is connecting to the system. Further the USB was scanned whether it consists of virus or not.

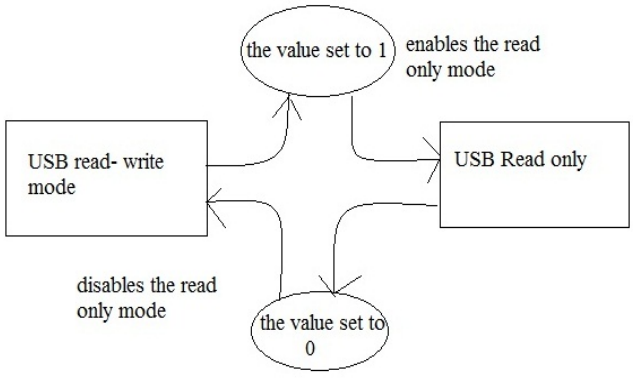

Fig 2 Enable or disable USB Read Only Mode

2.3 Deleting Replicated Virus In USB

In this module we are deleting the virus that are replicating to the system. So the virus are deleting not only in the infected pen drives, they are deleted in the infected system. We are searching for the virus that was replicated before and that was in the system. So we are detecting the virus and deleting it. After deleting the virus we are changing the USB into read and write only. Then we can access the USB safely without any malware. The USB was changed into write only mode. The value can be changed into 0 from 1 because the virus containing in the system was not to replicated into the USB further it will affect the other system when it is connected. We are providing the safety measures to the system that the virus shouldn't replicate to the system. There are some common viruses that are replicate to the system very easily. The main aim of this module is to delete the virus inside the USB pen drive without communicating with operating system. Finally in this module we are providing the virus that shouldn't be replicate to the system.

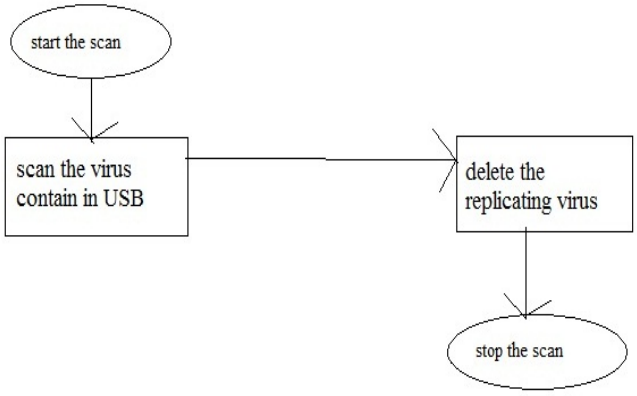

Fig 3 It is used to scan for replicating virus in the USB

III. SYSTEM ARCHITECTURE

This architecture tells about the how proposed system will work while it is implemented. At first, the pen drive is inserted into the computer, if the pen drive doesn't contain any virus, and then there is no need of scanning the content in the pen drive. If there is a virus in the computer then it will communicate with the application created in the system. The application provides the features to stop the autoplay features in the windows operating system. Then the autoplay feature will display the pen drive cannot open directly by the user when it was inserted. Then the USB pen drive changed into the USB read only mode hence the files in pen drive cannot be written by the infected files without knowledge of operating system. Hence the replication of virus can be stopped so the operating system stays safer from the virus [7]. Finally the pen drive is scanned by the scanner provided by the application. If the virus is found it was reported to the user knowledge. And some common replicated virus are deleted if it was contained in the pen drive. Then the pen drive can be used safely in the other system also [1]. The application can be run in the windows 7 operating systems.

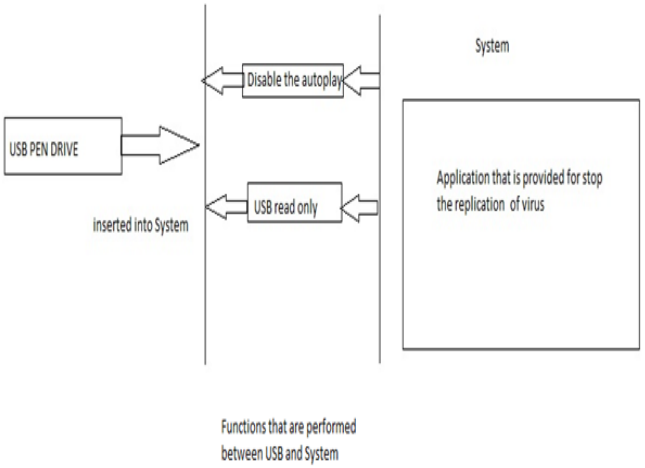

Fig 4 Operation Of Function Between The USB And System

IV. Results And Discussion

These features are done automatically where other software is not done. This may be simple concept but it may protect many users from the virus to their computers. When we compared to the anti-virus software they are provided for a fee with a feature that may allow the virus to attack sometimes. It may be become very difficult to remove from the computers. By disabling the autoplay feature, the virus can be stopped to replicate into the computers. The approached methods will provide the scanning the virus with the MD5 hashing techniques. Here the every single files are converted into MD5 hashing codes and they are compared with virus hashing codes which was stored previously. When the virus was detected, it will redirect to the result tab in that the detected virus is shown and it will delete from the System. This system will enable to download the file safely from the internet. This software was tested through the EICAR anti-malware test file. Previously antivirus software will not allow you to disable the autoplay features automatically. This software has additionally same changes in the existing anti-virus soft wares. This may stop the virus that attack through the USB to the computers. Here, in this software is developed for the Microsoft Windows operating systems

V. Conclusion

By creating the application with the features that are disabling the autoplay will reduce the virus attack to the computer [9]. Then, scanning virus by changing the features called USB read only mode. It makes USB secure from the attack of virus which is present in the computer. It allows the computer changes the values automatically by the software.

VI. Discussion

In this software, it can be developed by connecting with many anti-virus engines to the single software. When all engines are connected the software may be updated with virus definitions. The virus may be created daily it is very hard to protect the system. So the virus should perform the heuristic techniques to scan the viruses. The viruses are built strongly so the software can't stop strongly so the proposed system may protect the system at the risk level of a particular system. In future the application will developed inside the USB to interact with the operating systems. Automatically, the virus will delete inside the USB itself before connecting to the operating systems.

References

[1] McDowell, Mindi. "*Understanding Hidden Threats: Rootkits and Botnets*". US-CERT. 6 February 2013.

[2] Saumil shah, "*The anti-virus book*". The Tata McGraw-Hill publications.

[3] Jan Hruska, "*Computer Virus And Anti-virus Warfare*". Ellis Horwood, 1992.

[4] H. Poor, "A Hypertext History of Multiuser Dimensions," *MUD History*, http://www.ccs.neu.edu/home/pb/mud-history.html. 1986. (URL link *include year).

[5] Aycock, John "Computer *Viruses and Malware"*. Springer.2006.

[6] Grimes, Roger "*Malicious Mobile Code: Virus Protection for Windows"*. O'Reilly. 2001.

[7] Bishop, Matt. "*Computer Security: Art and Science*". Addison-Wesley Professional. 2003.

[8] Skoudis, Edward "*Infection mechanisms and targets*". Prentice Hall Professional.

[9] Polk, William T. "*Antivirus Tools and Techniques for Computer Systems"*. William Andrew.1995.

[10] Thomas Chen, Jean-Marc Robert . "*The Evolution of Viruses and Worms*.(http://vxheaven.org/lib/atc01.html), 2009.

[11] Zhang, Yu et al . "*A Novel Immune Based Approach For Detection of Windows PE Virus*". Springer. 2009

[12] Ludwig, Mark A. "*The Little Black Book of Computer Viruses: Volume* ". 2009.

[13] Rooney, Ben . "*Malware Is Posing Increasing Danger*". Wall Street Journal. 2011.

[14] Fred Cohen, "*Computer Viruses*", PhD Thesis, University of Southern California, ASP Press, 1988.